▶▶▶▶▶▶▶▶▶ 公平な金融システムの実現に向けて ～ Fintech プロジェクトの挑戦～ 研究プロジェクト

千葉商科大学政策情報学部 教授
研究プロジェクト代表
大矢野　潤
OYANO Jun

はじめに

1989 年、日本のコンピュータネットワークは全米科学財団ネットワーク（NSFNET）と IP 接続を開始した。日本におけるインターネットの始まりである。以来、インターネットは新聞や TV、百科事典、デパート、そして友人関係までも電子化し、その枠組みに取り込むことで社会基盤としての地位を確立してきた。しかし、私達の日常生活に欠かせないものであるにもかかわらず、これまで電子化できていないものがあった。意外にも、それは「お金（通貨）」である。

電子化されたお金、すなわち「仮想通貨」とはネットワーク上で用いられる流通性や汎用性を持つ電子的な決済手段の一つである。なお、2018 年 12 月に金融庁が公表した“「仮想通貨交換業等に関する研究会」報告書”では、法令上の呼称を「仮想通貨」から「暗号資産」に変更することが提案されたが、本稿においては引き続き仮想通貨という呼称を用いることにする。

日本の法定通貨である一万円札には一万円の価値があることを「国」が保証しているが、インターネットのように特定の国に属さない環境ではそのようなオーソリティを仮定しない決済手段が望まれる。もちろん、一般の電子商取引に仮想通貨が絶対に必要ということではない。例えば、信販会社のクレジットカードを用いてショッピングサイトで商品を購入する場合は、決済に至るまでの手続きをコーディングし、最終的なお金の移動をネットワーク外部の信販会社で行えばよい。ただし、この方法は送金に用いることができないこと、支払いが個人の信用情報に紐づけされてしまうなど、現金のもつ利便性、匿名性等の性質が失われてしまう。

インターネット上でのサービスを実現する場合、すべてのパーツから作り直すよりも既存のビジネスを連携させて新たな仕組みを構築する方が自然であろう。そして、ビジネス間の支払いは、より一般的で制約が少ない方法を検討したい。しかし、仮想通貨は安全な支払いを実現しているが、その支払いがビジネスの意図を反映しているかということは一切保証しない。我々は、一般のビジネス設計者が利用可能なビジネスロジックのテンプレートが必要であると考え、千葉商科大学経済研究所プロジェクト「安全で公平な金融システムの実現に資する Fintech フレームワークの提案」（以下、単に Fintech プロジェクト）を発足させた。期間は 2 年間、スタッフは 4 名の小さなプロジェクトである。目標が壮大すぎることは承知しているが、商科大学に勤務する情報・数理科学を専門とする研究者として、この問題を避けることができないという思いからの挑戦である。

以下、仮想通貨、支払いへの攻撃、ビジネスロジックの統合について簡単に説明し、最後に Fintech プロジェクトの現状と今後について報告する。

仮想通貨

ここでは、仮想通貨についての考え方を簡単に紹介する。なお、代表的な仮想通貨であるビットコインについての筆者による入門的な解説[1]が千葉商科大学の Web サーバで公開されている。仮想通貨に馴染みのない方はあらかじめ一読されたい。

オンラインショップで商品を購入する際、その支払い方法としてはクレジットカード、代引き、プリペイド式の電子マネーを用いるのが一般的であろう。インターネットを通じて行われた注文であっても、最終的な決済は外部サーバのデータを更新することで行われるため、いわゆる通貨のように電子データが「流通」するわけではない。

インターネット上に通貨と同様の仕組みを構築するための決定的な方法は最近まで知られていなかったが、2009 年、Satoshi Nakamoto による論文“Bitcoin: A Peer-to-Peer Electronic Cash System”[2]（以下、Satoshi Nakamoto 論文）で提案されたブロックチェーン（blockchain）が有力であると考えられている。同

論文において提案された電子通貨がいわゆるビットコイン（Bitcoin）であり、ビットコインにおける「電子コイン」とは「連続するデジタル署名のチェーン」と定義されている。つまり「電子コインが発行されてから現在までのコインの支払いの履歴記録」そのものがコインであり、この記録の最後に記録されているアドレスが現在のコインの所有者となる。コインの支払いは記録の最後に新しい所有者を付け加えることで行われるが、この手続きは、複数の暗号技術を駆使して実現されており、第三者による偽造や改ざんは困難である。

データの改ざんを防ぐための技術は電子署名としてビットコインよりも前から知られていた。問題は、コインの所有者が複数のアドレスに対して支払いを行う、いわゆる二重支払い（double spending）が可能なことであり、ブロックチェーンは二重支払い問題の現実解として提案された。二重支払いは結果として署名のチェーンの分岐を生成するが、ブロックチェーンではプルーフオブワーク（Proof Of Work）という仕組みを用いることで、分岐したチェーンの一方のみを正当なものであると「ネットワークが合意する」。「分散環境において、各々の通信主体が意図的であるかどうかにかかわらず間違った情報を伝達する可能性がある場合でも、ネットワーク全体として正しい合意を形成できるか」という問題はビザンチン将軍問題（Byzantine Generals Problem）と呼ばれ、1982 年に Leslie Lamport らによって定式化された[3]。ブロックチェーンはビザンチン将軍問題に対する一つの現実解を提示しているともいえる。

支払いへの攻撃

前述のとおり、ブロックチェーンはそれぞれの支払いの背景にある意図を考慮しない。例えば、ある商品の代金を、宛先が別のアドレスに書き換えられているのに気が付かずに送金してしまったとしても、ブロックチェーン上では正当な支払いとみなされる。意図に反して使用させられたコインを「これはそもそも自分のものだ」と主張して他の送金に再利用しても、ネットワークからは二重支払いとみなされ拒絶されてしまう。

一般に、ネットワーク上の手続き（以下、プロトコル）に欠陥がないことを証明することは非常に困難である。例えば Roger Needham と Michael Schroeder によって 1978 年に発表された Needham-Schroeder 公開鍵プロトコル[4]は、「安全でないネットワーク上で二人の参加者が相互に認証する」ための手続きを規定する。このプロトコルは発表以来17年間安全であると信じられていたが、1995 年に Gavin Lowe によってその脆弱性が指摘された[5]。二人の参加者のうち一人が「うっかり」侵略者に話しかけた結果、二人の秘密が侵略者に漏洩してしまう可能性が生じるのである。複数のビジネスロジックを組み合わせて新たなビジネスを生み出す作業においては、このような「うっかり」した状況を作り出す余地がないことを確認しなくてはならない。

ビジネスロジックの統合

複数の異なるビジネスロジックをシームレスに統合し、企業間のコラボレーションを促進しようとする動きは 2000 年台前半から盛んに行われてきた。代表的なものに、標準化団体 World Wide Web Consortium（W3C,https://www.w3.org/）による Web Services Choreography、OASIS（https://www.oasis-open.org/）による WS-BPEL などが知られている。

旅行業は企業間コラボレーションの代表例といってもよい。旅行は宿泊施設、交通手段、観光施設など複数の「旅行素材」を組み合わせたサービスであり、また、インターネットを介してユーザからの予約を受け付ける業態（Online Travel Agency）はすでに広く利用されている。経済産業省の「平成29年度我が国におけるデータ駆動型社会に係る基盤整備」[6]によれば、「BtoC-EC のサービス系分野において、最も市場規模が大きいのは旅行サービスであり、2017 年の BtoC-EC の市場規模は 3 兆 3,742 億円、前年比で 11.0% の伸びとなっている」とある。今後、ビジネスのオンライン統合化の動きは他の分野に広がっていくものと期待される。

このように、一部の先進的な業界においてはビジネスの統合化が進んでいるが、個人ベースで信用できない相手と取引をするのはとても危険である。例えば、A がオンラインショップを利用して品物を販売すること考えてみよう。販売者 A と購入予定者 B はお互いに面識がなく、お互いに相手を信用できないものとする。ここで、A が先に品物を送付すれば、B が品物を受け取り代金は送金しないリスクが発生する。逆に、B が代金を先払いした場合には、A が代金を受け取り品物は送付しないリスクが発生する。このため、「代引き」など適当なリスク回避手段が存在しない場合には、A と B の間で取引が開始されることはない。

この問題の解として、文献[7]に安全な遠隔取引（Safe Remote Purchase）アルゴリズムが公開されている。以下、簡単に説明しよう。

まず、A に 500 円の商品を販売する意思があり、B にはその商品を同じく 500 円で購入する意思があるものとする。この時、A、B は直接代金のやりとりをするのではなく、「仲介者」を介して売買手続きを行う。ただし、ここでの仲介者とは、Solidityを用いて実現され公開されている改ざん困難なプロセスであると仮定する。

(1) A が価格の 2 倍の 1000 円を仲介者に送金する［供託金＝ 1000 円］
(2) B が同じく 1000 円を仲介者に送金し、購買の意思を示す［供託金 =2000 円］
(3) A は B に品物を送付する［供託金 =2000 円］
(4) B は品物を受け取ったことを仲介者に知らせる［供託金 =2000 円］
(5) 仲介者は供託金から A に 1500 円、B に 500 円を返金する［供託金 =0 円］

ここで、上記のプロトコルがそれぞれのリスクに対する解となっていることを確認するのは容易である。A、B いずれかが代金や商品をだまし取ろうとしても、お互いに定価の倍の金額を供託しているため詐欺行為が割に合わないものになってしまっているのである。

ところで、このアルゴリズムは一般的なビジネスで通用するものであろうか？例えば中古車など定価が存在せず、支払い後の代金の金額に折り合いがつかない場合はどのように解決するであろうか？そもそも、A、B それぞれが代金の 2 倍の金額を供託する事は現実的なのであろうか？もちろん、取引相手の信用度を導入するなど、新たなプレーヤを投入する解法も存在するが、一般にそのプロトコルは複雑になり個人の手に負えなくなる。暗号システムのように、世界中の技術者によって提案とその検証がされ、安全性が確認されたものだけを適切に利用するといった仕組みが必要である。

Fintech プロジェクト

Web サービスとして記述されたビジネスプロセスに対する検証研究については、すでに様々な方法論が提案されている。細部において違いはあるものの、おおむね次のようなものであろう。

(1) WS-Choreography、WS-BPEL などに準拠したツールを用いてビジネスロジックを記述する
(2) ビジネスロジックをプロセス記述言語などの形式表現に変換する
(3) (2) で得られた形式表現を定理証明系、モデル検査器などを用いて検証する
(4) (4.1)検証に合格した場合は、その旨開発者に通知する
(4.2)検証に合格しなかった場合は、合格しなかった理由を表す反例を通知し、反例の解析を通じてビジネスロジックの理解を深める

Fintech プロジェクトでは、上記のアプローチに加え、次の点を考慮する。

- すでに「良い性質」が証明されている既存のビジネスプロセスを組み合わせて利用する
- 適当な抽象解釈を用いる

通常のビジネスロジックの設計者は既存のビジネスの「ユーザ」であり他社の提供するロジックに対して完全な証明を与える義務はないこと、証明論の知識がなくてもできる自動検証のためには複雑さ（状態数）を低く抑えるための抽象化が必要であるからである。

プロジェクトの現状と今後

2018 年 4 月、本プロジェクトが発足して以来すでに 9 ヶ月が経過した。この間、仮想通貨の現状を調査し、Satoshi Nakamoto 論文によるブロックチェーンの安全性を統計学的に確認、さらに、ビットコインと双璧をなす仮想通貨であるイーサリアム（Ethereum）の開発言語 Solidity についての理解を深めてきた。本プロジェクトにおけるビジネスロジック統合の具体例としてはブロックチェーン上で動作するボードゲームを予定している。ゲームのルールに複数のビジネスロジックを組み込み eLearning 教材として用いることを試みる。ビジネスゲームのプレーヤ（学生）は、ゲームのルールとしてビジネスロジックを理解し使いこなす必要がある。ゲームを活用した商業教育を実践し、経験を重ね、フィードバックしていくことで本プロジェクトのフレームワークの妥当性を検証する。

参考文献

1 大矢野潤 “「ビットコイン」って、いったい？”（2014 年） http://www.cuc.ac.jp/magazine/seisaku/news/2014/i8qio0000000yrum.html
2 Nakamoto, Satoshi.（2009 年 5 月 24 日）. “Bitcoin：APeer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf
3 Lamport, L.; Shostak, R.; Pease, M.（1982 年 7 月）. “The Byzantine Generals Problem”. ACM Transactions on Programming Languages and Systems4（3）：382-401. doi：10.1145/357172.357176.
4 Needham, Roger; Schroeder, Michael（December 1978）. “Using encryption for authentication in large networks of computers”. Communications of the ACM. 21（12）：993-999. doi：10.1145/359657.359659.
5 Lowe, Gavin（November 1995）. “An attack on the Needham-Schroeder public key authentication protocol”. Information Processing Letters. 56（3）：131-136. doi：10.1016/0020-0190(95)00144-2. Retrieved 2008-04-17.
6 経済産業省 商務情報政策局 情報経済課（2018 年 4 月）。“平成 29 年度 我が国におけるデータ駆動型社会に係る基盤整備” http://www.meti.go.jp/press/2018/04/20180425001/20180425001-2.pdf
7 “Safe Remote Purchase”. https://solidity.readthedocs.io/en/latest/solidity-by-example.html#safe-remote-purchase